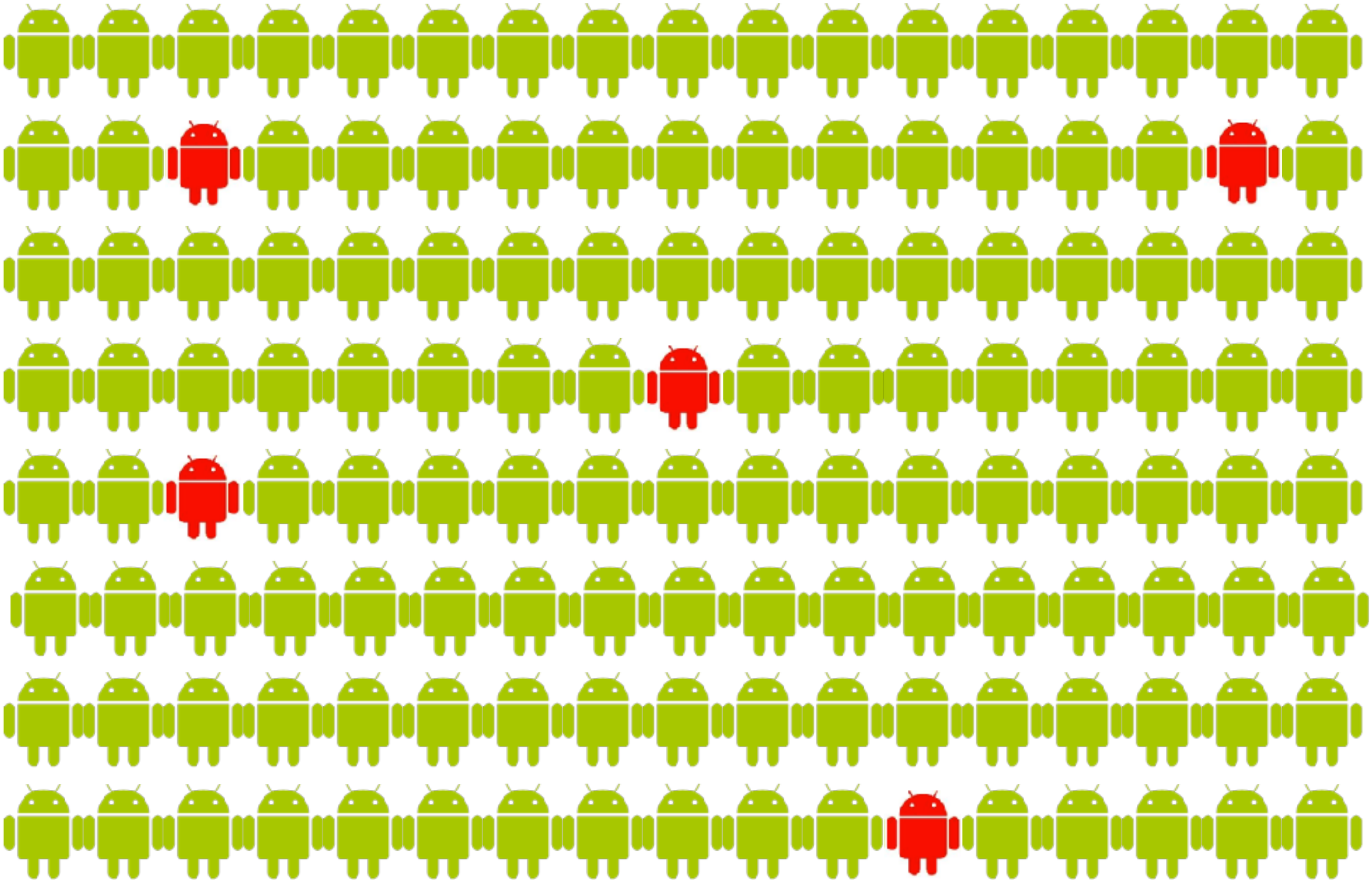
Making Malory Behave Maliciously: Targeted Fuzzing of Android Execution Environments

Siegfried Rasthofer, Steven Arzt, Stefan Triller
(Fraunhofer SIT, Germany)

Michael Pradel
(TU Darmstadt, Germany)

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT



TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

```
@Override
protected void onReceive(Bundle sms) {

    if(!sms.getBody.startsWith("ak40_1")){

        wait(24 hours);

        if(Build.FINGERPRINT.startsWith("generic"))
            return; // we are running in an emulator

        if(getCurrentLocation().equals("Germany")

            sendSMS(number, sms.getBody());

    }
}
```

Environment

?

Environment:

1. Send SMS to device
2. Content of SMS does not start with “ak40_1“
3. Wait for 24 hours
4. Run on real device
5. Location-Check for Germany

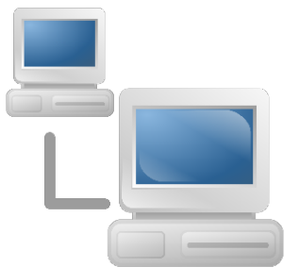
Dynamic Analysis?

Timing Bombs

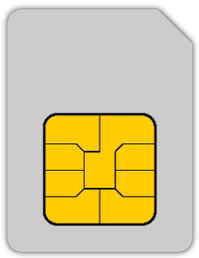
Emulator Checks

Country Checks

…



IP Restrictions



Provider Checks

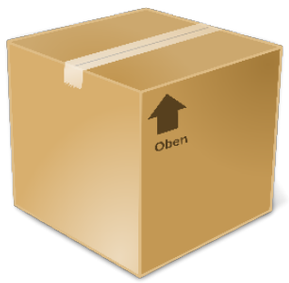
Integrity Checks

…

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

Static Analysis?



Packer

Reflection

…

Dynamic Codeloading

String Obfuscation

…

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

sendSMS(String, String)

Environment:

1. Send SMS to device
2. Content of SMS does not start with "ak40_1"
3. Wait for 24 hours
4. Run on real device
5. Location-Check for Germany

FuzzDroid

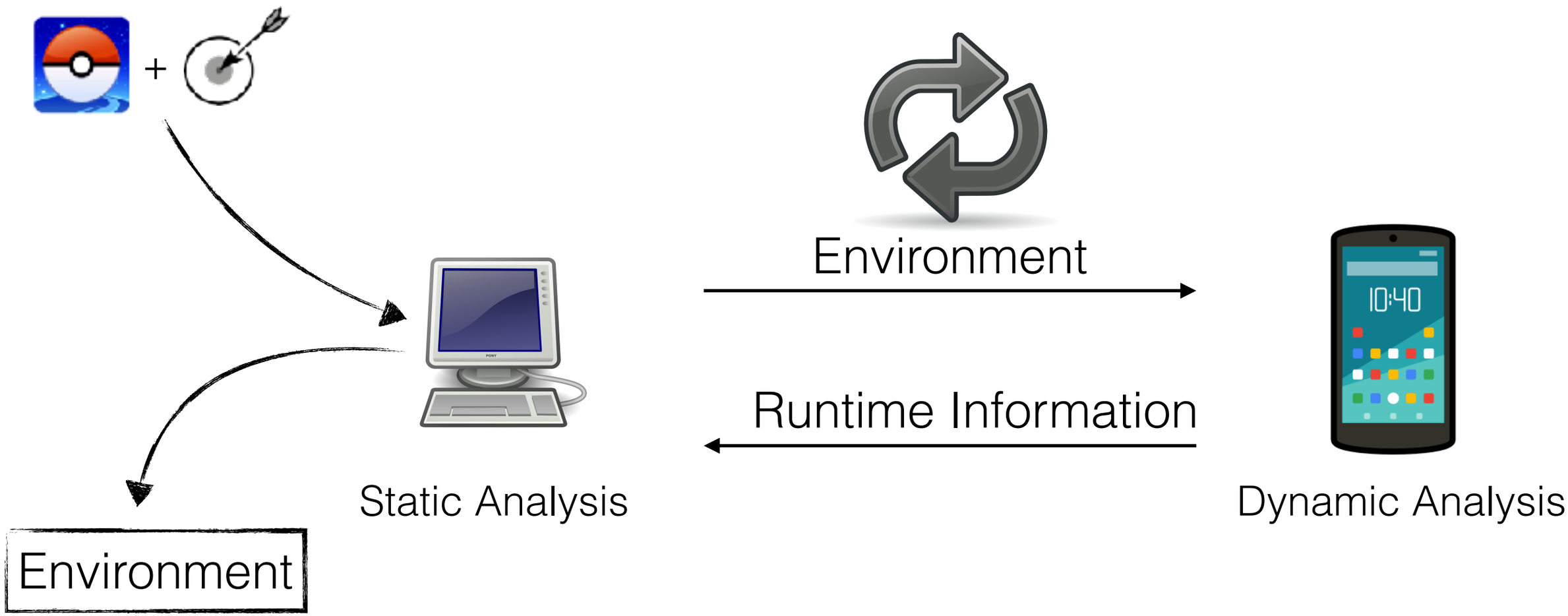
Static →  ← Dynamic

Targeted Fuzzing Approach

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

FuzzDroid



FINGERPRINT = "zte"

```
if(Build.FINGERPRINT.startsWith("generic"))
  return;
```

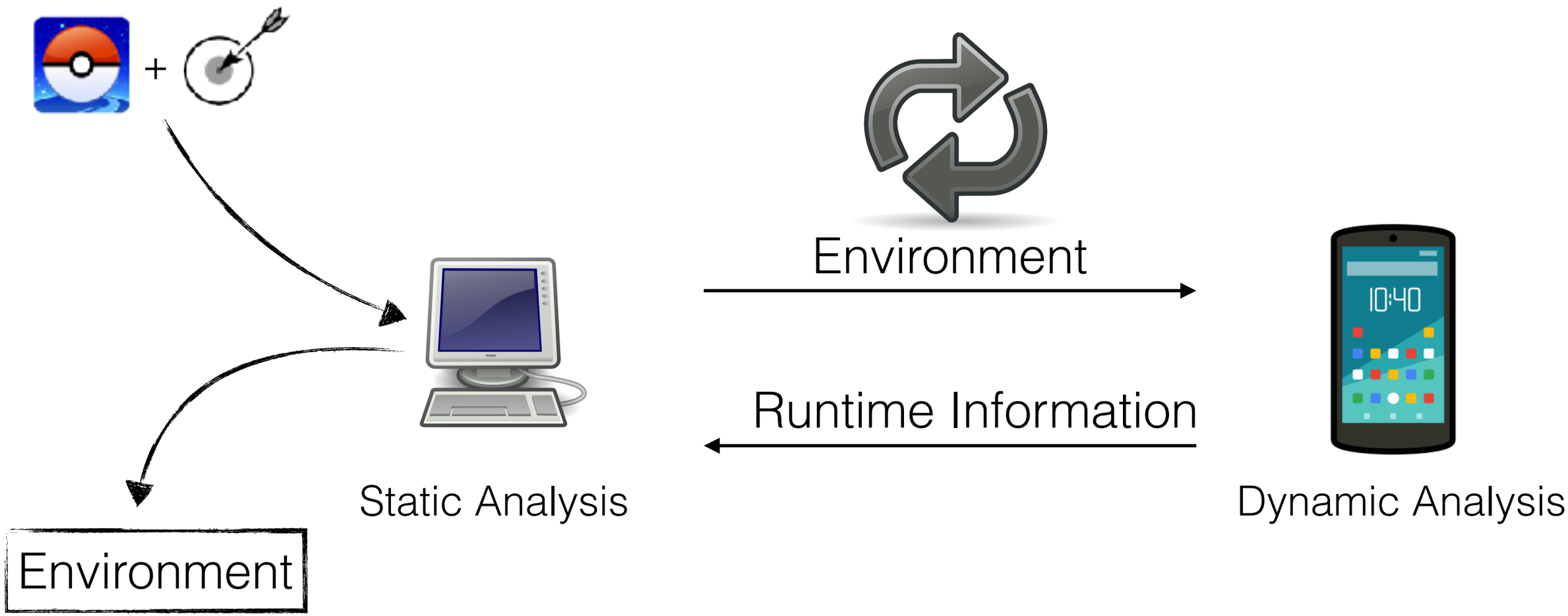
Location = "Argentina"

```
if(getCurrentLocation().equals("Germany")
  sendSMS(number, sms.getBody());
```


TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

FuzzDroid



✓ FINGERPRINT = "generic" →

```
if(Build.FINGERPRINT.startsWith("generic"))
  return;
```

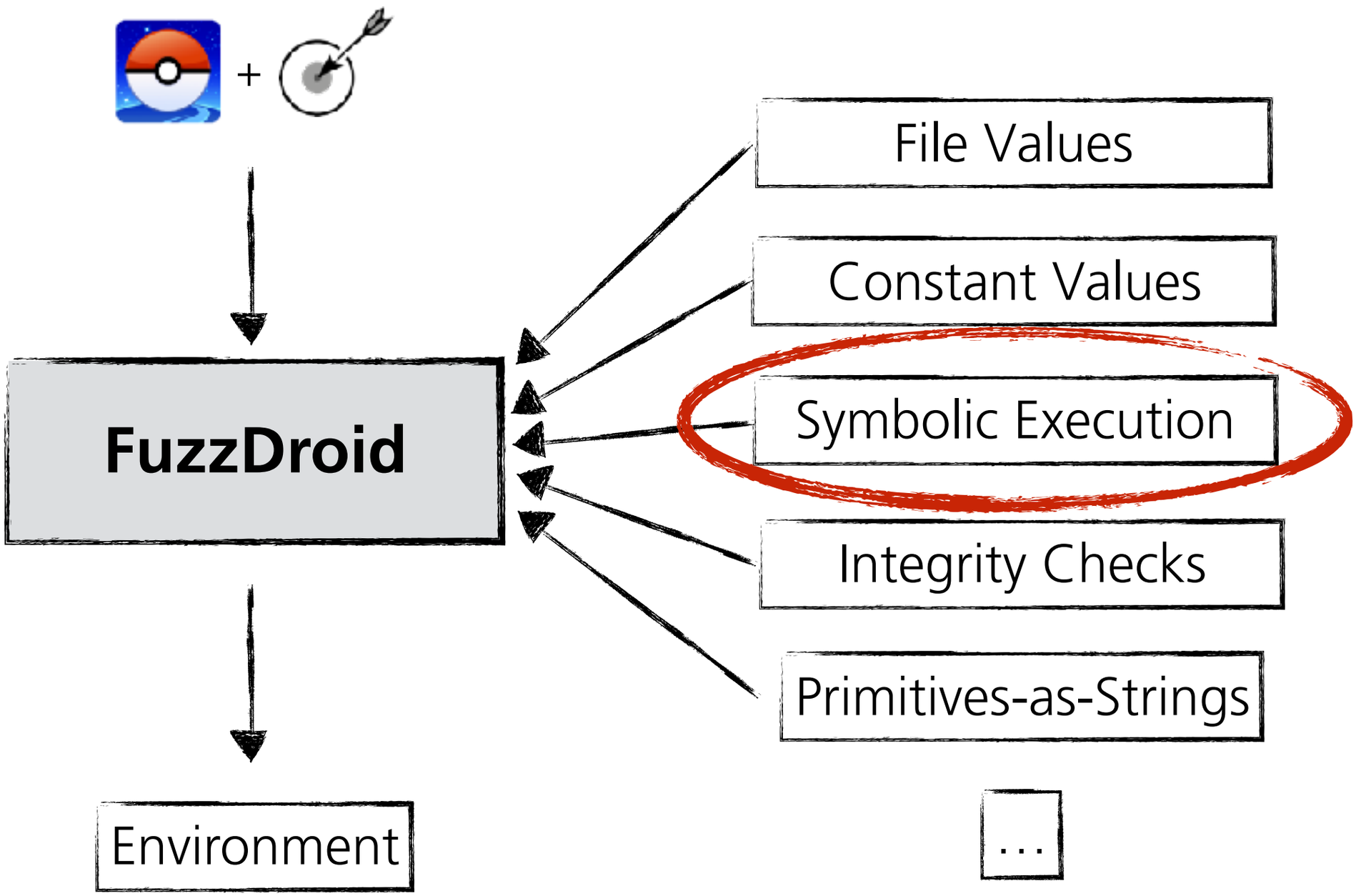
✓ Location = "Germany" →

```
if(getCurrentLocation().equals("Germany")
  sendSMS(number, sms.getBody());
```


TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

Value Provider



TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

Dataflow

```
a = getMessageBody()
```

↓

```
b = a
```

↓

```
c = b
```

↓

```
c.startsWith("ak40_1")
```

⇒

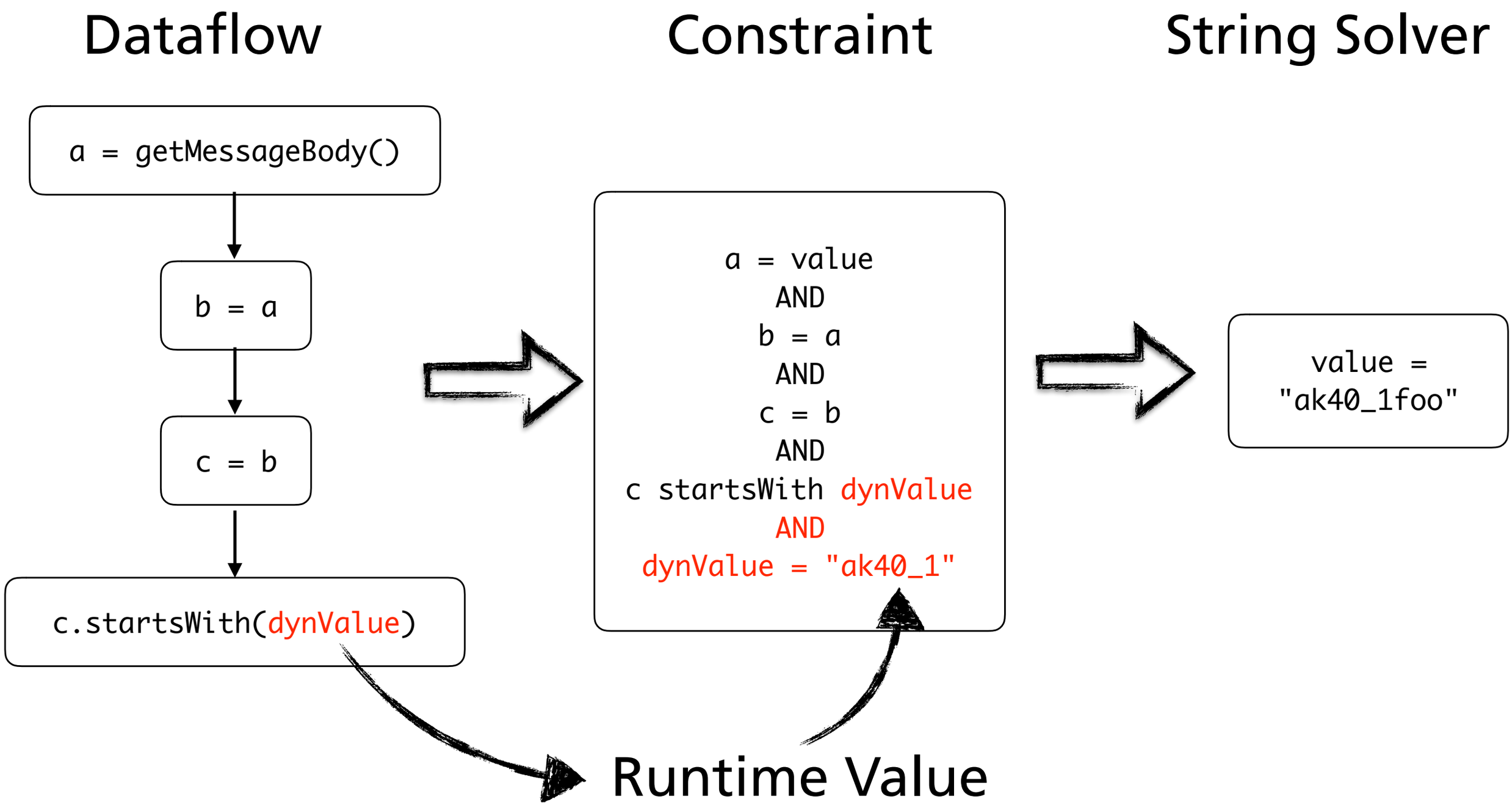
Constraint

```
a = value
  AND
b = a
  AND
c = b
  AND
c startsWith "ak40_1"
```

⇒

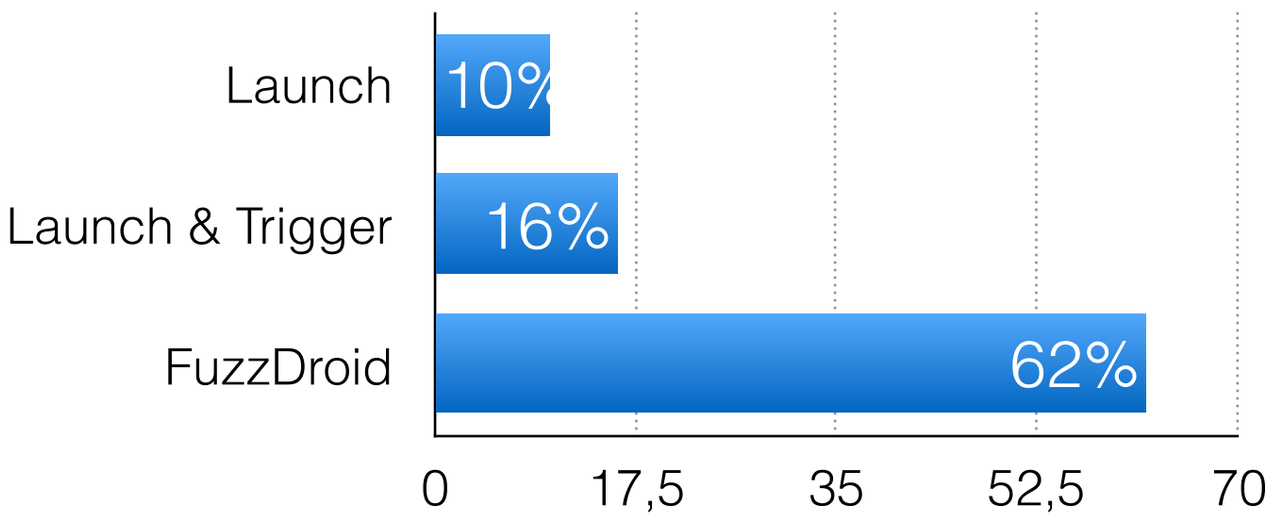
String Solver

```
value =
"ak40_1foo"
```

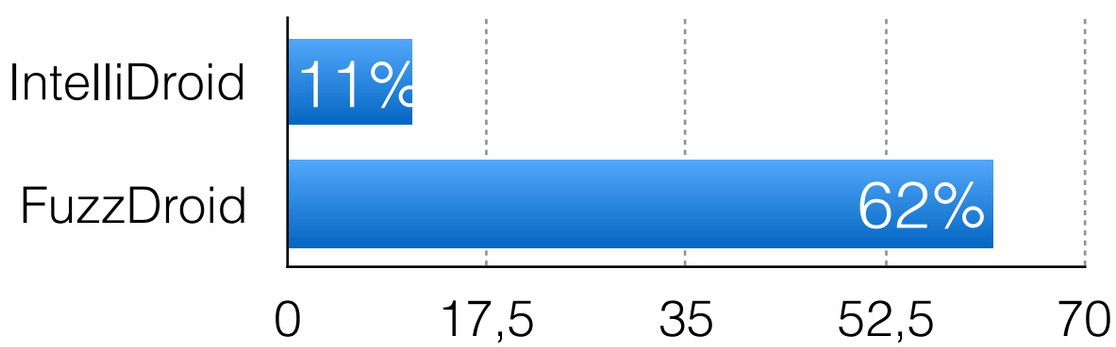

Dataflow
Constraint
String Solver
a = getMessageBody()
b = a
c = b
c.startsWith(dynValue)
a = value
AND
b = a
AND
c = b
AND
c startsWith dynValue
AND
dynValue = "ak40_1"
value =
"ak40_1foo"
Runtime Value

Evaluation

FuzzDroid Effectiveness?



209 Apps



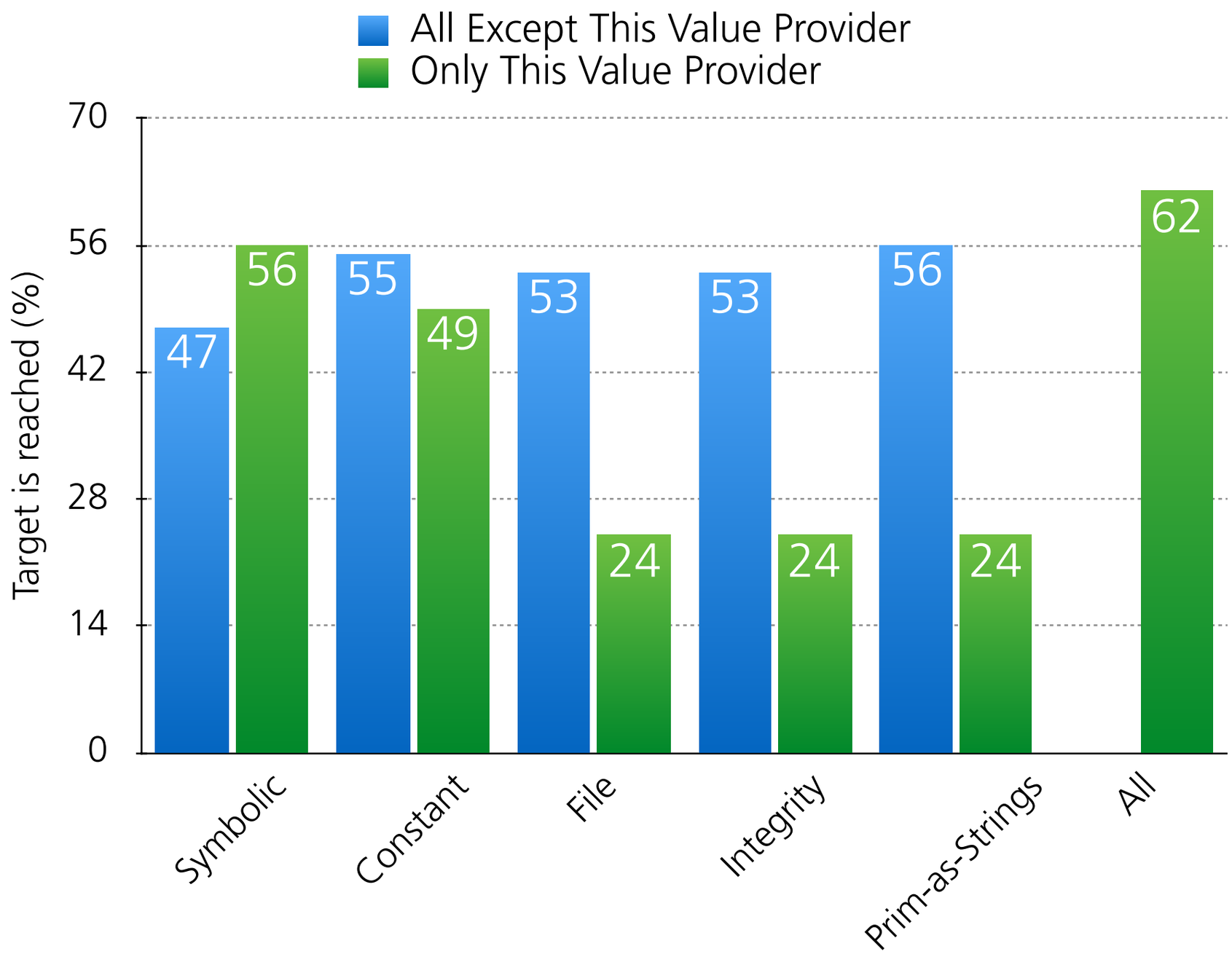
20 Apps

IntelliDroid: A Targeted Input Generator for the Dynamic Analysis of Android Malware. NDSS 2016

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

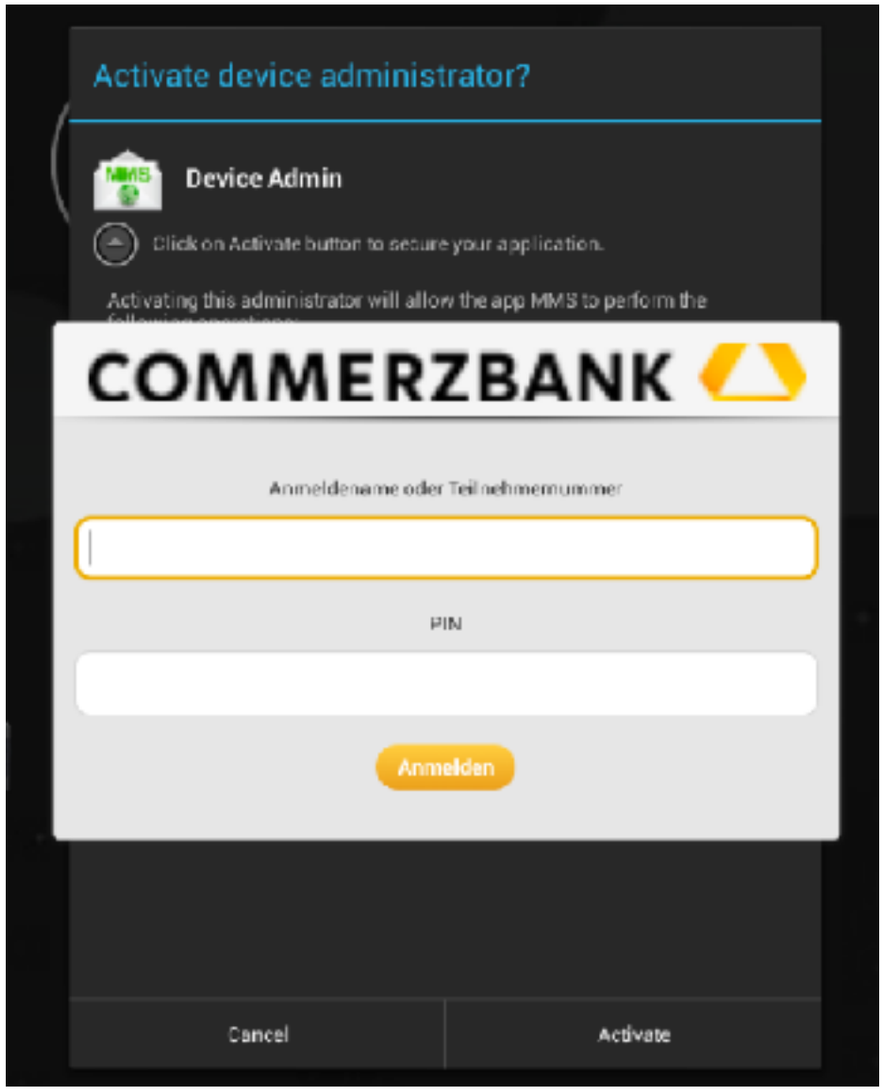
Multi-Analyses Effectiveness?



TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

Kind of environment	Prevalence
File Access	47.97 %
SIM/network operator code	16.82 %
Incoming SMS	10.84 %
SIM operator name	5.53 %
„Timing bomb“	4.06 %
SIM country	3.216 %
Integrity Check	1.02 %
Admin check	0.68 %
Others	9.92 %



TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

`sendSMS(String, String)`

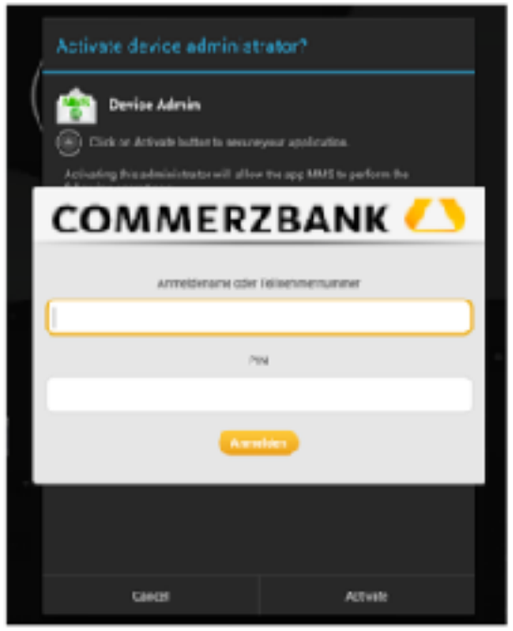
Environment:

1. Send SMS to device
2. Content of SMS does not start with "ak40_1"
3. Wait for 24 hours
4. Run on real device
5. Location-Check for Germany

FuzzDroid

Targeted Fuzzing Approach

Kind of environment	Prevalence
File Access	47.97 %
SIM/network operator code	16.82 %
Incoming SMS	10.84 %
SIM operator name	5.53 %
„Timing bomb"	4.06 %
SIM country	3.216 %
Integrity Check	1.02 %
Admin check	0.68 %
Others	9.92 %



TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

Fraunhofer
SIT

Siegfried Rasthofer

Fraunhofer Institute for
Secure Information Technology

siegfried.rasthofer@sit.fraunhofer.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer
SIT